CLAIMS:

1. A communication system comprising:

a first node;

a second node and;

at least one intermediate node between said first and second nodes;

wherein said first and second nodes are arranged to be in communication and said first and second nodes have a first security association and one of said at least one intermediate node and said second node have a second security association; and

wherein said first security association authenticates said second node to said first node and said second security association authenticates said at least one intermediate node to said second node.

2. A system as claimed in claim 1, wherein at least one of said first and second security associations comprise presenting at least one certificate to a respective one of said nodes for authentication.

3. A system as claimed in claim 2, wherein said at least one certificate comprises a cryptographic certificate.

4. A system as claimed in claim 3, wherein said certificate comprises an X.509 certificate.

5. A system as claimed in claim 1, wherein said at least one intermediate node inspects information sent between said first and second nodes.

6. A system as claimed in claim 1, wherein said at least one of intermediate nodes modifies information sent between said first and second nodes.

7. A system as claimed in claim 1, wherein said first node is attached to a wireless network.

8. A system as claimed claim 1, wherein said first node is attached to a packet switched network.

9. A system as claimed in claim 1, wherein said first node is attached to a network operating in accordance with a General Packet Radio System standard.

10. A system as claimed in claim 1, wherein said first node is connected to wireless user equipment.

11. A system as claimed in claim 10, wherein said first node comprises one of a plurality of first nodes connected to said wireless user equipment.

12. A system as claimed in claim 1, wherein said first node comprises a client device.

13. A system as claimed in claim 1, wherein at least one of said first and second security associations comprises encryption.

14. A system as claimed in claim 1, wherein said one of said at least one said intermediate node is configured to pass data packets from at least one of said first node to at least one of said second node and from at least one of said second node to at least one of said first node.

15. A system as claimed in claim 1, wherein said at least one intermediate node is arranged in a network gateway node.

16. A system as claimed in claim 15, wherein the network gateway node comprises one of a gateway GPRS support node and a serving GPRS support node.

17. A system as claimed in claim 15, wherein said second node is connected to said gateway node.

18. A system as claimed in claim 12, wherein said client device comprises a computer, user equipment, mobile station, or personal digital assistant.

19. A system as claimed in claim 1, wherein said second node comprises a server.

20. A system as claimed in claim 1, wherein said second node is configured to provide a service to said first node.

21. A system as claimed in claim 1, wherein the first node is configured to send a first connection message to the second node.

22. A system as claimed in claim 21, wherein said first connection message comprises a Transmission Control Protocol connection message.

23. A system as claimed in claim 1, wherein the first node is configured to send a hello message to the at least one intermediate node.

24. A system as claimed in claim 23, wherein said hello message comprises a Secure Socket Layer protocol handshake message.

25. A system as claimed in claim 23, wherein the at least one intermediate node is configured to make a copy of at least a part of said hello message.

26. A system as claimed in claim 23,, wherein said at least one intermediate node is configured to send said hello message to the second node.

27. A system as claimed in claim 1, wherein the second node is configured to send a hello message to the said at least one intermediate node.

28. A system as claimed claim 27, wherein said at least one intermediate node is configured to send a handshake message to the second node in response to receiving said hello message from said second node.

29. A system as claimed in claim 28, wherein said second node is configured to respond to said handshake message.

30. A system as claimed in claim 28, wherein said response comprises a Secure Socket Layer protocol handshake message.

31. A system as claimed in claim 28, wherein said handshake message sent to the second node comprises a Secure Socket Layer protocol handshake message.

32. A system as claimed in claim 28, wherein said handshake messages are configured to create said second security association.

33. A system as claimed in claim 28, wherein said handshake message sent by said one of said at least one intermediate node comprises a client certificate.

34. A system as claimed in claim 33, wherein said one of said at least one intermediate node is configured to create said client certificate when requested.

35. A system as claimed in claim 33, wherein said one of said at least one intermediate node is configured to retrieve said client certificate from a storage device.

36. A system as claimed in claim 1, wherein said at least one intermediate node and said second node are configured to generate at least one key to encrypt information sent between said at least one node and said second node, said at least one key being used in said second security association.

37. A system as claimed in claim 1, wherein said first node and said second node are configured to generate at least one key to encrypt information sent there between said first node and said second node, said at least one key being used in said first security association.

38. A system as claimed in claim 36, wherein said at least one intermediate node is configured to create said at least one key only when requested.

39. A system as claimed in claim 36, wherein said at least one intermediate node is configured to retrieve said at least one key from a storage device.

40. A system as claimed in claim 36, wherein said at least one key is configured to be dependent on a client certificate.

41. A system as claimed in claim 33, wherein at least one said client certificate certifies a known node which is known to said at least one intermediate node.

42. A system as claimed in claim 33, wherein said client certificate certifies a holder of a specified resource.

43. A system as claimed in claim 42, wherein said specified resource comprises one of an International Mobile Station Identity telephone number and a Mobile Station Integrated Service Digital Network telephone number.

44. A system as claimed in claim 42, wherein at least one said client certificate authorizes said second node to charge said holder of said specified resource for services used or purchased.

45. A system as claimed in claim 1, wherein said second security association is established before said first security association.

46. A system comprising:

a first node;

an intermediate node; and

a second node, wherein said intermediate node is configured to store security information for said first node, said security information being configured to be used to provide security for a connection between the intermediate node and said second node.

47. A system as claimed in claim 46, wherein said security comprises at least one of tunnelled connection, an authenticated connection and an encrypted connection.

48. A system as claimed in claim 46, wherein a common protocol is used between said first and second nodes.

49. An intermediate node for use in a system between a first node and a second node, said intermediate node being configured to at least one of to store and to generate security information relating to said first node.

50. A node as claimed in claim 49, wherein the security information comprises at least one of a security certificate, at least one security key, at least one public key and at least one private key.

51. A system as claimed in claim 49, wherein at least one intermediate node is configured to calculate a message digest based on a received data packet and a secret key.

52. A system as claimed in claim 51, wherein said at least one intermediate node adds said message digest to said received data packet prior to transmission.

53. A system as claimed in claim 52, wherein said message digest is configured to be bit-wise added to the received data packet.

54. A system as claimed in claim 52, wherein said message digest is configured to be concatenated to an end of the received data packet.

55. A system as claimed in claim 52, wherein said received data packet is configured to be encrypted by said secret key prior to being added to said message digest.

56. A system as claimed in claim 52, wherein said message digest is configured to be added to a final n bits of the received data packet.

57. A system as claimed in claim 52, wherein said message digest is configured to be calculated based on bits before the final n bits of the received data packet.

58. A system as claimed in claim 51, wherein said at least one intermediate node is configured to remove said message digest from said data packet.

59. A system as claimed in claim 51, wherein said at least one intermediate node is configured to decrypt said data packet using said secret key.

60. A system as claimed in claim 27, wherein said second security association is based on data within said hello message sent from said second node.

61. A system as claimed claim 1, wherein said first node comprises an Secure Socket Layer Client node.

62. A method for a communication system comprising a first end node, a second end node and at least one intermediate node positioned between said first and second end nodes, comprising the steps of:

applying a first security protocol to information sent between said first and second nodes; and

applying a second security protocol to information sent between one of said intermediate nodes and said second node, wherein the information is then sent to or from said first node.

63. A method for authenticating data packets in an intermediate node comprising the steps of:

receiving a data packet from a first node;

generating a secret key;

generating a message digest based on said data packet and said secret key;

generating a further data packet based on said data packet and said message digest; and

transmitting said further data packet to a second node.

64. The method of claim 63, wherein said step of generating said further packet comprises the step of bit wise adding the message digest to a selection of bits from said data packet.

65. The method of claim 63, wherein said step of generating said further packet comprises the step of concatenating the message digest to said data packet.

66. The method of claim 63, further comprising the step of encrypting said data packet by said secret key prior to said step of generating said message digest.

67. The method of claim 63, further comprising the step of encrypting said data packet by said secret key prior to said step of generating said further data packet.

68. The method of claim 63, wherein said receiving step comprises receiving said data packet being M bits long.

69. The method of claim 68, wherein said receiving step comprises selecting the last n bits of said data packet.

70. The method of claim 69, wherein said generating the message digest step depends on a first M-n bits of said data packet.

71. The method of claim 63, further comprising the steps of:

receiving a data packet from said second node;

generating a modified data packet by removing the message digest from said data packet from said second node; and

transmitting said modified data packet to said first node.